

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Special Agent (SA) Bradley Baker, being duly sworn, hereby state that the following is true to my knowledge and belief:

PRELIMINARY BACKGROUND INFORMATION

1. I am a Special Agent with Homeland Security Investigations (HSI), Department of Homeland Security (DHS) assigned to the Office of the Assistant Special Agent in Charge, Nogales, Arizona. I have been a criminal investigator with Homeland Security Investigations since 2018. I am a sworn federal law enforcement officer and have authority to investigate federal offenses pursuant to Title 18 of the United States Code. I am currently assigned to the Cyber Crimes Group, which conducts investigations of crimes where computers and the internet are used in the sexual exploitation of children, including (but not limited to) violations of 18 U.S.C. Sections 2252 and 2252A, which prohibit a person from knowingly transporting, receiving, distributing, possessing or accessing with intent to view, in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, child pornography, as defined in 18 U.S.C. Section 2256(8).

2. I am a graduate of the Criminal Investigator Training Program and the HSI Special Agent Academy at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. During the HSI Special Agent Academy, I received formal and on-the-job training in the investigation of cases involving the sexual exploitation of children to include training programs and participation in the execution of search warrants involving child pornography and seizures of computers and other storage media. I have also successfully completed the Internet Crimes Against Children (ICAC) BitTorrent Investigations, eMule Investigations, and Freenet Investigations courses held by the National Criminal Justice Training Center. I currently hold a CompTia A+ certification and have completed the Treasury Computer Forensic Training Program for Basic Computer Evidence Recovery Training (BCERT) and Basic Mobile Device Forensics (BMDF). I have completed multiple SANS courses and received a Global Information Assurance Certification (GIAC) in Security Essentials (GSEC) and iOS/macOS Examiner (GIME).

3. Prior to joining Homeland Security Investigations, I received a Bachelor of Science degree in Criminal Justice from Appalachian State University and then became a Special Agent with North Carolina State Bureau of Investigation Alcohol Law Enforcement Branch for more than eight (8) years in Asheville, North Carolina. During that time, I conducted numerous criminal investigations involving violations of criminal laws resulting

in arrests. During these investigations, I applied for and executed numerous search warrants that resulted in successful prosecutions. I was also a Federal Task Force Officer with Homeland Security Investigations for two years. During that time, I became familiar with and assisted with the enforcement of federal laws. The statements contained in this Affidavit are based on my experience and background as a special agent as well as on the training and information provided by other law enforcement agents.

4. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

5. This investigation concerns alleged violations of 18 U.S.C. §§ 2252 and 2252A, relating to material involving the sexual exploitation of minors. 18 U.S.C. §§ 2252 and 2252A prohibit a person from knowingly transporting, receiving, distributing, possessing, or accessing with intent to view, in interstate or foreign commerce, or using any facility or means of interstate or foreign commerce, any visual depictions of minors engaging in sexually explicit conduct (child pornography) as defined in 18 U.S.C. Section 2256(8).

6. I am submitting this Affidavit under Rule 41 of the Federal Rules of Criminal Procedure in support of an Application for a Search Warrant authorizing a search of a Seagate 1TB Portable Hard Drive with serial number: NAC2D6WT (SUBJECT DEVICE).

7. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess or knowingly access with intent to view, child pornography.

8. I am requesting that the court issue a search warrant directed to search the SUBJECT DEVICE to locate child pornography and conclusively identify the user(s) possessing child pornography.

9. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish

probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252 and 2252A are located on the SUBJECT DEVICE.

10. To my knowledge, no prior attempt by investigative or legal process has been submitted to obtain the same or similar information sought in this warrant application. The SUBJECT of the investigation is likely unaware of the existence of this investigation, has not been contacted, and therefore has made no statements to the effect that he would preserve the original data in lieu of seizure.

PERTINENT FEDERAL CRIMINAL STATUTES

11. This investigation concerns alleged violations of 18 U.S.C. §§ 2252 and 2252A, relating to material involving the sexual exploitation of minors.

12. 18 U.S.C. Sections 2252 and 2252A prohibit a person from knowingly transporting, receiving, distributing, possessing or accessing with intent to view, in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (child pornography) as defined in 18 U.S.C. Section 2256(8).

DEFINITIONS

13. The following non-exhaustive list of definitions applies to this Affidavit and Attachments A and B:

a. Child Pornography is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

b. Child Erotica means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not, in and of themselves, obscene or illegal. In contrast to "child pornography," this material does not necessarily depict minors in sexually explicit poses or positions. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writing, and diaries. *See Kenneth V. Lanning, Child Molesters: A Behavioral Analysis* (2001) at 65. Federal courts have recognized the evidentiary value of child erotica and its admissibility

in child pornography cases. *See United States v. Cross*, 928 F.2d 1030 (11th Cir. 1991) (testimony about persons deriving sexual satisfaction from and collecting non-sexual photographs of children admissible to show intent and explain actions of defendant); *United States v. Caldwell*, No. 97-5618, 1999 WL 238655 (E.D. Ky. Apr. 13, 1999) (child erotica admissible under Federal Rule of Evidence 404(b) to show knowledge or intent).

c. Visual depictions include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

d. Minor means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

e. Sexually explicit conduct means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

f. Computer means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1).

g. Computer hardware consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices), peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic or other digital form. It commonly includes computer operating systems, applications and utilities.

i. Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software or other related items.

j. Computer passwords and data security devices consist of information or items designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to unlock particular data security devices. Data security hardware may include encryption devices, chips and circuit boards. Data security software of digital code may include programming code that creates test keys or hot keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or booby-trap protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. Internet Service Providers or ISPs are commercial organizations, which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or coaxial cable data transmission, dedicated circuits or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name such as a username or screen name, an e-mail address, and an e-mail mailbox and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a coaxial cable system and can access the Internet by using his or her account name and password.

l. ISP Records are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

m. Internet Protocol address or IP address refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a subscriber's computer at varying intervals at the discretion of the ISP. IP addresses might also be static meaning an ISP assigns a user's computer a specific IP address which is used each time the computer accesses the Internet.

n. The terms records, documents and materials include all information recorded in any form, visual or aural, and by any means, whether in hand-made form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, printing and/or typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

o. Digital device includes any electronic system or device capable of storing, processing, interpreting or rendering data in digital form, including computer systems of various form factors (computer desktop systems, towers, servers, laptops, notebooks and netbooks), personal digital assistants, cellular telephones and smart phones, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors and drives intended for removable media; related communication devices such as wired and wireless home routers and modems; storage media such as electro-mechanical hard disks, solid state hard disks, hybrid hard disks, floppy disks, optical disks such as compact disks and digital video disks, magnetic tapes and volatile and non-volatile solid state flash memory chips; and security devices including dongles and flash chips.

p. Image or copy refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. Imaging or copying maintains contents, but attributes may change during the reproduction.

q. Hash value refers to a value generated after data has been subjected to a cryptographic mathematical algorithm. A hash value is akin to a digital fingerprint in that dissimilar data will not produce the same hash value after being subjected to the same hash algorithm. Therefore, a hash value is particular to the data from which the hash value was

generated. Known hash values can be used to search for identical data stored on various digital devices and/or media as identical data will have the same hash value.

r. Compressed file refers to a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY AND ONLINE CHILD EXPLOITATION

14. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet since approximately 1997. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

15. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. Computer technology and the Internet revolutionized the way in which child pornography is produced, distributed, stored and communicated as a commodity and a further tool of child exploitation. For instance:

a. Individuals can transfer photographs from a camera onto a computer-readable format with a variety of devices, including scanners, memory card readers, or directly from digital cameras, including those on most cellphones.

b. Modems allow computers to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

c. The capability of a computer to store images in digital form makes the computer itself an ideal repository for child pornography. As explained further below, the storage capacity of electronic media used in home computers has increased tremendously within the last several years. These drives can store an extreme amount of visual images at very high resolution.

d. The Internet, the World Wide Web, and other Internet components afford individuals many different and relatively secure and anonymous venues for obtaining,

viewing, and trading child pornography, or for communicating with others to do so or to entice children.

e. Individuals can use online resources to retrieve, store, and share child pornography, including services offered by Internet Portals such as Google, America Online (AOL), Yahoo!, and Hotmail, among others. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. And even in cases where online storage is used, evidence of child pornography can be found on the user's computer in most cases.

f. As is the case with most digital technology, computer communications can be saved or stored on hardware and computer storage media used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite web sites in, for example, bookmarked files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or footprints in the web cache and history files of the browser used. Such information is often maintained for very long periods of time until overwritten by other data.

g. The interaction between software applications and the computer operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a computer hard drive without the user's knowledge. Even if the computer user is sophisticated and understands this automatic storage of information on his computer's hard drive, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the computer media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's computer media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution and possession of child pornography.

h. Data that exists on a computer is particularly resilient to deletion. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available

forensic tools. When a person deletes a file on a home computer, the data contained in the file does not actually disappear, rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space, that is, in space on the hard drive that is not allocated to an active file and is left unused and free to store new data. Such residual data may remain in free space for long periods of time before it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity and computer habits.

BACKGROUND ON COMPUTERS AND EVIDENCE ASSESSMENT PROCESS IN CHILD PORNOGRAPHY AND CHILD EXPLOITATION INVESTIGATION

16. This warrant seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes how computers were used, the purpose of their use, and who used them.

17. As described above and in Attachment B, this application seeks permission to search and seize certain records that might be found on the SUBJECT DEVICE, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. In addition to user-generated documents (such as word processor, picture and movie files), computer hard drives can contain other forms of electronic evidence that are not user-generated. In particular, a computer hard drive may contain records of how a computer has been used, the purposes for which it was used and who has used these records, as described further in the attachments. Further, in finding evidence of how a computer has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present on a hard drive or that a particular person (in the case of a multi-user computer) was not a user of the computer during the time(s) of the criminal activity. For instance, based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that when a computer has more than one user, files can contain information indicating the dates and times that files were created as

well as the sequence in which they were created, so that evidence of whether a user accessed other information close in time to the file creation dates, times and sequences can help establish user identity and exclude other users from computer usage during relevant times.

18. Because the absence of particular data on a digital device may provide evidence of how a digital device has been used, what it has been used for, and who has used it, analysis of the digital device as a whole may be required to demonstrate the absence of particular data. Such evidence of the absence of particular data on a digital device is not segregable from the digital device.

19. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a computer user, and contextual evidence excluding a computer user. All of these types of evidence may indicate ownership, knowledge, and intent. This type of evidence is not “data” that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

SEARCH METHODOLOGY TO BE EMPLOYED

20. Consistent with the information provided within this affidavit, contextual information necessary to understand the evidence, to identify the user/possessor of the child pornography, and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.

21. Additional techniques to be employed in analyzing the seized items will include (1) surveying various file directories and the individual files they contain; (2) opening files to determine their contents; (3) scanning storage areas, (4) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in this affidavit and its attachments, and (5) performing any other data analysis techniques that may be necessary to locate and retrieve the evidence described in this affidavit and its attachments.

22. Because it is expected that the SUBJECT DEVICE may constitute (1) an instrumentality of the offense, or contain (2) fruit of criminal activity, (3) contraband, or (4) evidence otherwise unlawfully possessed, it is anticipated that such evidence will not be returned to the owner and that it will be either forfeited or ultimately destroyed in accordance with the law at the conclusion of the case. However, if after careful inspection investigators determine that the device does not contain (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence of the person who committed the offense and under what circumstances the offense was committed, then such items seized will be returned.

DETAILS OF THE INVESTIGATION

23. On November 12, 2020, Siegfried FUHRMANN was indicted by a federal grand jury in the District of Arizona for one count of 18 U.S.C. 1594(c) and 1591, Conspiracy to Commit Sex Trafficking of Minors, eight counts of 18 U.S.C. 1591(a) and 1591(b)(2), Sex Trafficking of a Minor, one count of 18 U.S.C. 2423(c), Engaging in Illicit Sexual Conduct in a Foreign Place, one count of 18 U.S.C. 2423(b), Travel with Intent to Engage in Illicit Sexual Conduct, one count of 18 U.S.C. 2251(c), Production of Child Pornography, and one count of 18 U.S.C. 2251A(b), Selling or Buying Children. FUHRMANN is currently pending a sentencing hearing and was placed on pre-trial release.

24. FUHRMANN was placed on Pre-trial Release, with conditions that included restrictions on using unmonitored computers and not committing any new crimes. I was informed by his pre-trial officer that his own computer was monitored, and his wife's was not.

25. On or about April 19, 2023, I was notified by pre-trial services that FUHRMANN was suspected of having used his wife's computer to view child sex abuse material. On April 20, 2023, I interviewed Angie and Randy Kayfew, daughter and son-in-law of FUHRMANN. During the interview, the Kayfews indicated that Ingrid Fuhrmann, wife of FUHRMANN, had recently undergone back surgery and was in the hospital from March 29 through April 6, 2023. The Kayfews stated that after Ingrid returned home from the hospital, she observed pornography on the computer screen while FUHRMANN was using her Dell computer.

26. R. Kayfew informed me that on April 19, 2023, he traveled to Ingrid and FUHRMANN's residence, 12397 N Wing Shadow Lane, Marana, Arizona. While at the residence, R. Kayfew inspected Ingrid's Dell desktop computer and observed what he

described as child pornography. R. Kayfew said he found approximately two to three dozen pictures/videos inside the downloads folder on the computer. R. Kayfew described some of the pictures as what he believed to be an eight-year-old female having sex with a dog and a male. R. Kayfew also remembered seeing a file name of “young daughter and beast.” R. Kayfew also explained that the date stamps associated with these files were April 2, 2023.

27. I traveled to FUHRMANN’s residence and met with Ingrid. Ingrid informed me that FUHRMANN’s computer was monitored by pretrial services, and he was not allowed to be on her Dell desktop computer. Ingrid told me that her Dell computer requires a password to log on and she had not provided that to FUHRMANN. Ingrid informed me that on April 6, 2023, the day she returned home from the hospital, FUHRMANN used her Dell computer in her presence, and she observed “kiddie porn” on the computer screen. Ingrid provided SA Baker with written consent to search her Dell desktop computer.

28. HSI SA Richard Koch and I conducted a consent search of the Dell computer utilizing the forensic tool osTriage. I located numerous files of interest, but most appear to be computer-generated imagery (CGI) appearing to depict children. Several files depicted what appear to be computer-generated images of female children under the age of eighteen engaged in sexual activity. Some of these files also showed these minor females engaging in sexual activity with dogs or horses.

29. For example, an image with file name “1-95-2.jpg” depicted a CGI image of a completely nude prepubescent female child approximately seven to ten years of age performing oral sex on a male dog. The female child has what appears to be semen on her anus, vagina, stomach, and mouth.

30. The osTriage report detailed that several of the CGI files of interest had a file path beginning with the drive letter “F:”, and the majority were last accessed between the dates of April 2, 2023, and April 6, 2023. At the time of the consent search there was not a drive connected to the Dell computer that was assigned the letter “F:”

31. The osTriage report showed that on April 6, 2023, at 12:44:58 p.m., a Seagate USB attached mass storage device was connected to the Dell computer. The report listed the Seagate storage device as having a serial number of NAC2D6WT (SUBJECT DEVICE). The report then showed this device was disconnected from the Dell computer at 4:49:54 p.m. on the same day. Ingrid stated she did not have a Seagate portable hard

drive. The osTriage report did not show any other USB storage devices that had been connected to the Dell computer.

32. After I departed the residence, I received a phone call from R. Kayfew informing me he located the SUBJECT DEVICE inside FUHRMANN's residence. I traveled to FUHRMANN's residence and met with R. Kayfew. R. Kayfew handed me the SUBJECT DEVICE and I confirmed the serial number printed on the device as the same listed in the osTriage report. I seized the SUBJECT DEVICE.

33. During a forensic review of the Dell desktop computer, I located images depicting minors engaging in sexually explicit conduct which were not computer-generated, in addition to the CGI files depicting virtual children. Numerous images depicting a known child victim engaging in sexual acts with FUHRMANN were discovered. During a previous forensic interview of this child victim, she stated she was fourteen (14) years of age during her sexual interactions with FUHRMANN. Several of the pictures show FUHRMANN penetrating the victim's vagina with his fingers and engaging in sexual intercourse. For example, one image depicts the child victim completely nude laying on her back on a bed. A male wearing boxers with flames, FUHRMANN, can be seen inserting his penis into the child's vagina.

RETURN AND REVIEW PROCEDURES

34. Pursuant to Rule 41 of the Federal Rules of Criminal Procedure, I understand and will act in accordance with the following:

a. Pursuant to Rule 41(e)(2)(A)(i), an agent is required to file with the court an inventory return, that is, an itemized list of the property seized, within fourteen (14) days of the execution of the warrant.

b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized or copied on-site after the issuance of the warrant, not the later review of the media or information seized, or the later off-site digital copying of that media.

c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the physical storage media that was seized or copied, not an itemization of the information or data stored on the physical storage media. Under Rule 41(f)(1)(B), I may retain a copy of that information for purposes of the investigation. The government intends to make and retain a full image copy of the seized media, so that a copy of the evidence, rather than the original evidence, can be examined. The government

will seize and retain both the original evidence and any copies of this evidence. This procedure will ensure that the original evidence remains intact and that potential child pornography and instrumentalities of such crime will not be returned to the subject.

CONCLUSION

35. Based on the foregoing, I believe that there is probable cause that the SUBJECT DEVICE contains evidence in violation of Title 18 U.S.C. §§ 2252 and 2252A, which, among other things, makes it a federal crime for any person to produce, possess, receive, distribute or knowingly access with intent to view child pornography, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located in the SUBJECT DEVICE, as more fully described in Attachment A.

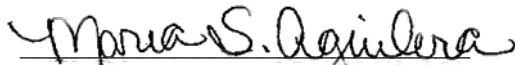
Respectfully submitted,

BRADLEY
D BAKER

Digitally signed by
BRADLEY D BAKER
Date: 2023.04.27
10:31:55 -07'00'

Bradley Baker
Special Agent – HSI

Telephonically subscribed and sworn before me this 27th of April, 2023


The Honorable Maria S. Aguilera
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF THE PROPERTY TO BE SEARCHED

A Seagate 1TB Portable Hard Drive with serial number: NAC2D6WT



ATTACHMENT B
ITEMS TO BE SEARCHED AND SEIZED

1. All records, contained in the SUBJECT DEVICE and all internal memory therein, that relate to violations of 18 U.S.C. §§ 2252 and 2252A including:
 - a. Stored photographs, videos or any images of minors;
 - b. Any hidden, deleted or erased data, communications, graphical images, multimedia items or documents found in the subject devices, which constitute evidence of the offenses listed above;
 - c. Evidence of who used, owned, or controlled the subject device at the time the things described in this warrant were created, received, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - d. Contextual information necessary to understand the evidence described in this attachment;
 - e. Records of Internet activity, including but not limited to caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user typed web addresses.
 - f. Images of child pornography and files containing images of child pornography, in any form, wherever they may be stored or found within the SUBJECT DEVICE.
2. Any and all software, including programs to run operating systems, applications, utilities, compilers, interpreters, and communications programs, including, but not limited to, P2P software.
3. Information, correspondence, records, documents, or other materials pertaining to the possession, receipt or distribution of child pornography, or sexual interest in children, that were transmitted or received, including:
 - a. Correspondence, including electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, child pornography; and

- b. Records bearing on the productions, reproduction, receipt, shipment, orders, requests, trades, purchases or transactions of any kind involving the transmission through interstate or foreign commerce including by U.S. mail or by computer of child pornography;
 - c. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet to purchase, sell, trade transmit or acquire child pornography. These records may include ISP records, i.e., billing and subscriber records, chat room logs, and e-mail messages.
 - d. Any and address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
 - e. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
 - f. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography or sexual conduct involving children.
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
5. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

6. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to ownership of the items described above.
7. Any and all computer software or applications that may be utilized to create, receive, distribute, store, modify, or destroy any of the evidence sought.
8. Evidence of software that would allow others to control the SUBJECT DEVICE, such as viruses, Trojan horses, and other forms of malicious software;
9. Evidence of the lack of such malicious software;
10. Evidence of the times the SUBJECT DEVICE was used; and
11. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT DEVICE.
12. Evidence of who used, owned, or controlled the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved usernames and passwords, documents, and browsing history;